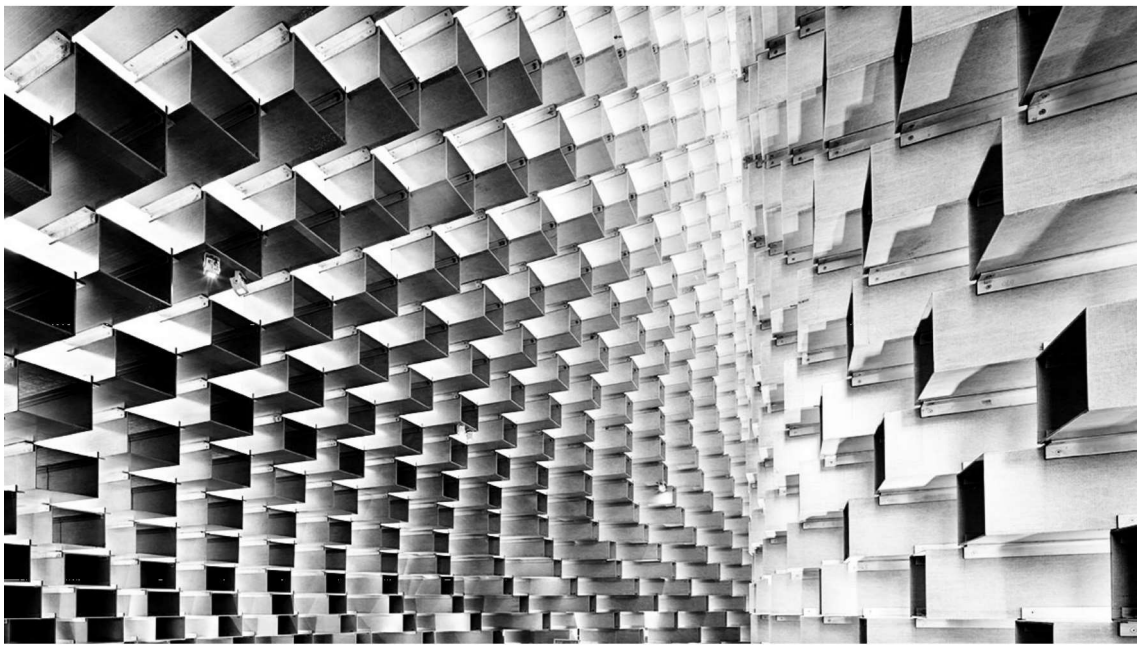
Harvard
Business
Review

Technology

A Brief History of Blockchain

by Vinay Gupta

February 28, 2017



Many of the technologies we now take for granted were quiet revolutions in their time. Just think about how much smartphones have changed the way we live and work. It used to be that when people were out of the office, they were *gone,* because a telephone was tied to a place, not to a person. Now we have global nomads building new businesses straight from their phones. And to think: Smartphones have been around for merely a decade.

We're now in the midst of another quiet revolution: blockchain, a distributed database that maintains a continuously growing list of ordered records, called "blocks." Consider what's happened in just the past 10 years:

INSIGHT CENTER

Business in the Era of Blockchain

How technology is transforming transactions.

- The first major blockchain innovation was bitcoin, a digital currency experiment. The market cap of bitcoin now hovers between $10–$20 billion dollars, and is used by millions of people for payments, including a large and growing remittances market.
- The second innovation was called blockchain, which was essentially the realization that the underlying technology that operated bitcoin could be separated from the currency and used for all kinds of other interorganizational cooperation. Almost every major financial institution in the world is doing blockchain research at the moment, and 15% of banks are expected to be using blockchain in 2017.
- The third innovation was called the "smart contract," embodied in a second-generation blockchain system called ethereum, which built little computer programs directly into blockchain that allowed financial instruments, like loans or bonds, to be represented, rather than only the cash-like tokens of the bitcoin. The ethereum smart contract platform now has a market cap of around a billion dollars, with hundreds of projects headed toward the market.
- The fourth major innovation, the current cutting edge of blockchain thinking, is called "proof of stake." Current generation blockchains are secured by "proof of work," in which the group with the largest total computing power makes the decisions. These groups are called "miners" and operate vast data centers to provide this security, in exchange for cryptocurrency payments. The new systems do away with these data centers, replacing them with complex financial instruments, for a similar or even higher degree

of security. Proof-of-stake systems are expected to go live later this year.

- The fifth major innovation on the horizon is called blockchain scaling. Right now, in the blockchain world, every computer in the network processes every transaction. This is slow. A scaled blockchain accelerates the process, without sacrificing security, by figuring out how many computers are necessary to validate each transaction and dividing up the work efficiently. To manage this without compromising the legendary security and robustness of blockchain is a difficult problem, but not an intractable one. A scaled blockchain is expected to be fast enough to power the internet of things and go head-to-head with the major payment middlemen (VISA and SWIFT) of the banking world.

This innovation landscape represents just 10 years of work by an elite group of computer scientists, cryptographers, and mathematicians. As the full potential of these breakthroughs hits society, things are sure to get a little weird. Self-driving cars and drones will use blockchains to pay for services like charging stations and landing pads. International currency transfers will go from taking days to an hour, and then to a few minutes, with a higher degree of reliability than the current system has been able to manage.

These changes, and others, represent a pervasive lowering of transaction costs. When transaction costs drop past invisible thresholds, there will be sudden, dramatic, hard-to-predict aggregations and disaggregations of existing business models. For example, auctions used to be narrow and local, rather than universal and global, as they are now on sites like eBay. As the costs of reaching people dropped, there was a sudden change in the system. Blockchain is reasonably expected to trigger as many of these cascades as e-commerce has done since it was invented, in the late 1990s.

Predicting what direction it will all take is hard. Did anybody see social media coming? Who would have predicted that clicking on our friends' faces would replace time spent in front of the TV? Predictors

usually overestimate how fast things will happen and underestimate the long-term impacts. But the sense of scale inside the blockchain industry is that the changes coming will be "as large as the original invention of the internet," and this may not be overstated. What we can predict is that as blockchain matures and more people catch on to this new mode of collaboration, it will extend into everything from supply chains to provably fair internet dating (eliminating the possibility of fake profiles and other underhanded techniques). And given how far blockchain come in 10 years, perhaps the future could indeed arrive sooner than any of us think.

Until the late 1990s it was impossible to process a credit card securely on the internet — e-commerce simply did not exist. How fast could blockchain bring about another revolutionary change? Consider that Dubai's blockchain strategy (disclosure: I designed it) is to issue all government documents on blockchain by 2020, with substantial initial projects just announced to go live this year. The Internet of Agreements concept presented at the World Government Summit builds on this strategy to envision a substantial transformation of global trade, using blockchains to smooth out some of the bumps caused by Brexit and the recent U.S. withdrawal from the Trans-Pacific Partnership. These ambitious agendas will have to be proven in practice, but the expectation in Dubai is that cost savings and innovation benefits will more than justify the cost of experimentation. As Mariana Mazzucato teaches in *The Entrepreneurial State*, the cutting edge of innovation, particularly in infrastructure, is often in the hands of the state, and that seems destined to be true in the blockchain space.

Vinay Gupta is the founder of Hexayurt.Capital, a fund which invests in creating the Internet of Agreements. He was instrumental in creating the Dubai Blockchain Strategy, project managed the Ethereum blockchain platform release, and invented the hexayurt refugee shelter. His areas of expertise include disaster management, energy policy, and computer graphics.